

[0141] The end systems timing server and slave shall have their IPsec policy defined such that a dedicated IPsec tunnel with authentication (AH) and encryption (ESP) support shall be established. The tunnel shall have a limited lifetime and shall be refreshed from time to time as needed. Both end systems of the tunnel shall have the SPI associated with tunnel used for transferring ToP packets, but it is unknown other nodes in the larger network, this will help mitigate various man-in-the-middle attacks. The anonymity for the ToP packets can further be enhanced by adding random amount (variable) padding to the IPsec payload (at the tail end of the ToP packets carried in IPsec tunnel).

[0142] As discussed, we use exclusive SA (Security Association) for 1588 traffic and unique SPIs (Security Parameter Index) for 1588 traffic, though this use is for example and not limiting.

[0143] Our method introduces delay/jitter because of the IPsec. However, the time need to encrypt the timing messages is not a constant. Thus, the offset would also not be a constant. To remedy the variance of offset values, over various iterations the offset times are collected, perhaps in a table, and these values are entered into a histogram to find a mean value. With this mean value the timing can be regulated more accurately. In other words, a statistical mean of the value of the latency is created such that an average offset based on a running average can be created to add to t_3 .

[0144] Therefore, we perform statistical analysis on the edge timestamp offset to estimate the internal security provisioning delay on egress path.

[0145] In the ingress path 400, also shown in FIG. 4A, when the packet arrives it is decrypted and after decryption the timestamp t_2 is applied by the timing module. A tabulation may be made as shown in FIG. 4B.

[0146] At a receiving node, an encrypted timing message enters 402. In our example, the timing message is an IPsec message in ESP tunnel mode. This tunnel is solely for the use of such timing messages, such that the tunnel is exclusive to the encrypted timing messages. When the encrypted message exits the tunnel, only then can it be decrypted 404. The decrypted message is then time stamped upon arrival at the ToP timing solution module 406. The anonymity for the timing packets can further be enhanced by adding random amount (variable) padding to the IPsec payload (at the tail end of the ToP packets carried in IPsec tunnel).

[0147] Egress (or transmitting end) 1588 in IPsec will put a statistically estimated edge timestamp offset ($t_1'-t_1$ for SYNC; $t_3'-t_3$ for Delay_Req) in the Residence Time field before SYNC and Delay_Req are encrypted in IPsec ESP payload, allowing the ToP slave clock Servo algorithm to offset the delay/jitter introduced by IPsec for 1588 ToP egress packets.

[0148] The timestamp assigned by timing module for egress packets (t) $t=t_3+(\text{estimated offset})$, where t_3 is the time the packet leaves the timing module and where t_3' is the time packet reaches PHY after encryption by IPsec engine. The time t_3' and associated packet ID (P) are sent to the s/w on SoC for collating the packet and calculating the offset for creating distribution. The times are tabulated, for example, as shown in FIG. 4C.

[0149] A mean of ($t_3'-t_3$) from the distribution will give the mean offset value t that can be used to find the estimated

offset in the path due to encryption. The mean can be determined, for example, by the use of a histogram, as shown in FIG. 4D.

[0150] The distribution calculates running/moving mean of the offset based on egress 1588v2 packets. Distribution of offset to determine mean estimated offset for large sample.

[0151] Additionally, the estimated offset t is periodically passed to the timing module to correct the time-stamp for inner packet by adding to original time t_3 .

[0152] Also, the timing module needs to maintain mapping of packet ID (outer/encrypted to time t_3'). Only the SoC has this outer to inner packet ID mapping and needs to be maintained to collate time per sample.

[0153] SPIO'. is sent to PHY upon change to PHY/DPI over MDIO by SoC IPsec engine.

[0154] Referring to FIG. 3 again and following the path of the encrypted message, this instance a time stamp module, for example, the time stamp module 327 associated with the ToP slave module 343 timestamps t_3 . Then the message is encrypted and just before it exits the node, now designated as the transmitting node, the time stamp module 329 records the time that the encrypted message exits, designated as t_3' .

[0155] FIG. 5 is a flow diagram of an example of an embodiment of the determining the offset from the egress side.

[0156] At a transmitting node, an unencrypted timing message originated at a clock 502 and is timestamped 504. The message is then encrypted 506. In our example, the timing message is encrypted as an IPsec message in ESP tunnel mode. This tunnel is solely for the use of such timing messages, such that the tunnel is exclusive to the encrypted timing messages. When the encrypted message leaves the transmitting node, a time stamp records that exit 508. For general purposes, we can refer to the time the unencrypted message is created as t_T for transmitted time. The time is the startpoint. When the encrypted message enters the tunnel, it is already encrypted. Therefore, the message itself cannot be timestamped. Rather, the exit time is recorded. We can refer to that time as t_T' for transmitted time prime. The offset caused by needing to encrypt the message is calculated as the t_T-t_T' or in other words, the difference between the final arrival time and the time the encrypted message entered the receiving node. Hence the offset is calculated 510.

[0157] As discussed herein, the offset time will vary upon each use. So each time a message is transmitted, those individual offset times as calculated need to be tabulated 512. Putting these values into a histogram, a mean offset time can be determined 514, which allows for a running average to be determined 516.

[0158] The anonymity for the timing packets can further be enhanced by adding random amount (variable) padding to the IPsec payload (at the tail end of the ToP packets carried in IPsec tunnel).

[0159] FIG. 6 also depicts an exemplary embodiment of the ingress path method.

[0160] FIG. 7 also depicts an exemplary embodiment of the egress path method.

[0161] The figures generally, and FIG. 3, FIG. 6, and FIG. 7 in particular, can also serve as providing an example of a system to secure timing synchronization to network nodes connected over an inherently insecure best effort public network with mechanisms to improve accuracy of timing protocols such as a statistically estimated edge timestamp offset encoded into the timing message to account for